

# **BLOCKCHAIN CLOUD BANKING: SECURE AND FAULT-TOLERANT TRANSACTIONS**

Submitted in partial fulfillment of the requirements for the award of  
Bachelor of Engineering Degree in Computer Science and  
Engineering

By

**NAVANEETH P(Reg.No-40110838)**

**G BALAJI BHARATH(Reg.No-40110146)**



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING  
SCHOOL OF COMPUTING**

## **SATHYABAMA**

**INSTITUTE OF SCIENCE AND TECHNOLOGY  
(DEEMED TO BE UNIVERSITY)**

**CATEGORY-1 UNIVERSITY BY UGC**

**Accredited with Grade "A++" by NAAC 12B Status by UGC  
Approved by AICTE  
JEPPIAAR NAGAR, RAJIV GANDHISALAI, CHENNAI - 600119**

**APRIL- 2024**



# SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Category - I University by UGC

Accredited "A++" by NAAC | Approved by AICTE

[www.sathyabama.ac.in](http://www.sathyabama.ac.in)

## DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

### BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **NAVANEETH P (40110838)** and **G BALAJI BHARATH (40110146)** who carried out the project entitled "**BLOCKCHAIN CLOUD BANKING: SECURE AND FAULT-TOLERANT TRANSACTIONS**" under my supervision from November 2023 to April 2024.

*D. Nancy*  
Internal Guide

Ms.D.Nancy Kirupanithi, MTech.,

*[Signature]*  
HEAD OF THE DEPARTMENT  
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING  
**SATHYABAMA**  
INSTITUTE OF SCIENCE AND TECHNOLOGY  
(DEEMED TO BE UNIVERSITY)  
Jeppiaar Nagar, Rajiv Gandhi Salai,  
Chennai - 600 119.

Submitted for Viva Voice Examination held on 18/04/2024.

*[Signature]*  
12/4/24  
Internal Examiner

*[Signature]*  
12/4/2024  
External Examiner

## DECLARATION

I, **G BALAJI BHARATH**(Reg.No-40110146) hereby declare that the Project Report entitled "**BLOCKCHAIN CLOUD BANKING: SECURE AND FAULT-TOLERANT TRANSACTIONS**" done by us under the guidance of **Ms.D.Nancy Kirupanithi, MTech.**, at Sathyabama Institute of Science and Technology is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering degree in Computer Science and Engineering.

DATE: 12/04/2024

PLACE: CHENNAI

G. Bx:

SIGNATURE OF THE CANDIDATE

## ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **Board of management of Sathyabama Institute of Science and Technology** for their kind encouragement in doing this project and for completing it successfully. We are grateful to them.

I convey my thanks to **Dr. T. Sasikala, M.E., Ph.D., Dean**, School of Computing, **Dr.L.Lakshmanan, M.E.,Ph.D.**, Heads of the Department, Department of Computer Science and Engineering for providing us the necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to our ProjectGuide **Ms.D.Nancy Kirupanithi, MTech.**, for her valuable guidance, suggestions and constant paved the way for the successful completion of my project work.

I wish to express my thanks to all teaching and Non-teaching staff members of the **Department of Computer Science and Engineering** who were helpful in many ways for the completion of project.

## **ABSTRACT**

Nowadays, large amounts of data are stored with cloud service providers. Third-party auditors (TPAs), with the help of cryptography, are often used to verify this data. Cloud Data Auditing Techniques with a Focus on Privacy and Security. It aims to provide a resource based on-demand. It avoids the online usage burden of accessing data through internet. Cloud storage supports to maintain data securely in cloud. Cloud is interconnected with group of computers, which is used to store information and run their applications in cloud platform. Through cloud computing, we can access any file, document of user from anywhere in the world. Mainly, cloud can be used for cost savings, high scalability and large storage space. But a major issues in cloud computing is security. Third-party auditors (TPAs) play a crucial role in verifying the integrity of data through cryptographic techniques, thus enhancing the security of cloud storage. This paper explores various cloud data auditing techniques with a focus on privacy and security, highlighting the importance of robust auditing mechanisms in maintaining data integrity and confidentiality. By providing a comprehensive resource on-demand, cloud data auditing helps mitigate security risks and ensures that data remains secure and accessible from anywhere in the world.

## TABLE OF CONTENTS

| CHAPTER NO | TITLE                                                      | PAGE NO    |
|------------|------------------------------------------------------------|------------|
|            | <b>ABSTRACT</b>                                            | <b>v</b>   |
|            | <b>LIST OF FIGURES</b>                                     | <b>vii</b> |
| <b>1</b>   | <b>INTRODUCTION</b>                                        | <b>1</b>   |
| <b>2</b>   | <b>LITERATURE SURVEY</b>                                   | <b>3</b>   |
|            | 2.1 Inferences from literature survey                      | <b>3</b>   |
|            | 2.2 Open problems in existing system                       | <b>6</b>   |
| <b>3</b>   | <b>AIM AND SCOPE OF THE PRESENT INVESTIGATION</b>          | <b>10</b>  |
|            | 3.1 Aim                                                    | <b>10</b>  |
|            | 3.2 Project Scope                                          | <b>10</b>  |
|            | 3.3 Risk analysis of the project                           | <b>11</b>  |
|            | 3.4 Software and hardware requirements                     | <b>14</b>  |
| <b>4</b>   | <b>EXPERIMENTAL MATERIALS AND METHODS; ALGORITHMS USED</b> | <b>15</b>  |
|            | 4.1 MODULE DESCRIPTION                                     | <b>16</b>  |
|            | 4.1.1 Admin Module                                         | <b>16</b>  |
|            | 4.1.2 TPAModule                                            | <b>16</b>  |
|            | 4.1.3 User Module                                          | <b>17</b>  |
|            | 4.1.4 Block Verification Module                            | <b>17</b>  |

|          |                                               |    |
|----------|-----------------------------------------------|----|
|          | 4.1.5BlockInsertionModule                     | 17 |
|          | 4.1.6BlockDeletionModule                      | 17 |
|          | 4.2SYSTEM ARCHITECTURE                        | 24 |
|          | 4.3DESCRIPTIONOFSOFTWAREFOR<br>IMPLEMENTATION | 25 |
| <b>5</b> | <b>RESULTSANDDISCUSSION</b>                   | 34 |
|          | 5.1RESULTS                                    | 34 |
| <b>6</b> | <b>SUMMARYANDCONCLUSION</b>                   | 38 |
|          | 6.1CONCLUSION                                 | 38 |
|          | <b>REFERENCES</b>                             | 39 |
|          | <b>APPENDIX</b>                               | 40 |
|          | <b>A.SOURCE CODE</b>                          | 46 |
|          | <b>B.SCREENSHOTS</b>                          | 53 |
|          | <b>C.RESEARCHPAPER</b>                        | 56 |

## LISTOFFIGURES

| FIGURENO. | FIGURENAME                | PAGENO. |
|-----------|---------------------------|---------|
| 4.1.1     | ClassDiagram              | 15      |
| 4.1.2     | UsecaseDiagram            | 17      |
| 4.1.3     | SequenceDiagram           | 18      |
| 4.1.4     | ComponentDiagram          | 20      |
| 4.1.5     | Activity Diagram          | 21      |
| 4.2       | SystemArchitectureDiagram | 23      |
| 5.1       | Login Page                | 34      |
| 5.2       | ClientRegistration        | 35      |
| 5.3       | Upload File               | 35      |
| 5.4       | FileSendingMetaKey        | 36      |
| 5.5       | Secret Key                | 36      |
| 5.6       | DownloadHistory           | 37      |

# CHAPTER1

## INTRODUCTION

Storing large amounts of data with cloud service providers (CSPs) raises concerns about data protection. Data integrity and privacy can be lost because of the physical movement of data from one place to another by the cloud administrator, malware, dishonest cloud providers, or other malicious users who might distort the data.<sup>1</sup> Hence, saved data corrections must be verified at regular intervals.

Nowadays, with the help of cryptography, verification of remote (cloud) data is performed by third-party auditors (TPAs). TPAs are also appropriate for public auditing, offering auditing services with more powerful computational and communication abilities than regular users.<sup>3</sup> In public auditing, a TPA is designated to check the correctness of cloud data without retrieving the entire dataset from the CSP. However, most auditing schemes don't protect user data from TPAs; hence, the integrity and privacy of user data are lost. Our research focuses on cryptographic algorithms for cloud data auditing and the integrity and privacy issues that these algorithms face. Many approaches have been proposed in the literature to protect integrity and privacy; they're generally classified according to data's various states: static, dynamic, multi owner, multiuser, and so on.

We provide a systematic guide to the current literature regarding comprehensive methodologies. We not only identify and categorize the different approaches to cloud data integrity and privacy but also compare and analyze their relative merits. For example, our research lists the

strengths and weaknesses of earlier work on cloud auditing, which will enable researchers to design new methods. Although related topics such as providing security to the cloud are beyond this article's scope, cloud data auditing requires explicit attention.

It represents the fusion of cutting-edge technologies in finance. Blockchain, renowned for its robust security and decentralized ledger system, intertwines with cloud-based banking, leveraging the scalability and accessibility of cloud computing. This integration promises a paradigm shift in financial operations by ensuring airtight security measures while enabling seamless transactions. The utilization of blockchain within cloud banking not only guarantees a high level of protection for sensitive financial data but also fortifies the system against potential faults or disruptions. This title encapsulates a forward-looking approach to banking, embracing innovation to deliver a trustworthy, resilient, and efficient platform for conducting transactions in the modern digital age.

## **CHAPTER 2**

### **LITERATURE SURVEY**

Literature survey is the most important step in any kind of research. Before we start developing, we need to study the previous papers of our domain which we are working and on the basis of study we can predict or generate the drawback and start working with the reference of previous papers.

#### **INFERENCES FROM LITERATURE SURVEY**

**TITLE: Cloud Data Auditing Techniques with a Focus on Privacy and Security**

**Author/Year: Omkar S, Shruthika H, Amit A/2019**

**Description:**

Nowadays, large amounts of data are stored with cloud service providers. Third-party auditors (TPAs), with the help of cryptography, are often used to verify this data. However, most auditing schemes don't protect cloud user data from TPAs. A review of the state of the art and research in cloud data auditing techniques highlights integrity and privacy challenges, current solutions, and future research directions.

**TITLE: A survey on auditing techniques used for preserving privacy of data stored on cloud:**

**Author/Year: Riya Sudam Bote, Shikha Virendar Chandel/2022 Description:**

Providing security to the stored data on the cloud is one of the important challenges in cloud computing. Encrypted data which is stored on the cloud may be viewed or modified by the cloud service provider. To overcome this problem many techniques have been developed but, those cannot guarantee accurately about the security of the stored data. These modifications of the data by the service provider or by others should also be known to the data owner. For such purpose, data tagging technique can be used to audit the data. Auditing is done by using Third Party Auditor (TPA). TPA stores data information of the data owner and challenges to the cloud server, depending upon the data owner request. With the help of such mechanism, TPA can convince both, data owner and cloud server.

**TITLE: Auditing in Cloud Computing Solutions with OpenStack**

**Author/Year: Anjali Sanjivanrao More, Deepa Sunil Ranaware / 2019**

**Description:**

This presentation will walk through how auditing works in a Cloud environment. We will touch upon things like Cloud Auditing Data standard (CADF), the auditing challenges in a distributed cloud platform like OpenStack and how they are overcome using by CADF.

**TITLE: Cloud Security Auditing Challenges and Emerging Approaches**

**Author/Year: Venkata Sasank Pagolu, Ganapathi Panda / 2021**

**Description:**

IT auditors collect information on an organization's information systems, practices, and operations and critically analyze the information for improvement. One of the primary goals of an IT audit is to determine if the information system and its maintainers are meeting both the legal expectations of protecting customer data and the company standards of achieving financial success against various security threats. These goals are still relevant in the newly emerging cloud computing model of business, but they need customization. There are clear differences between cloud and traditional IT security auditing. In this article, the authors explore potential challenges unique to cloud security auditing; examine additional challenges specific to particular cloud computing domains such as banking, medical, and government sectors; and present emerging cloud-specific security auditing approaches and provide critical analysis.

**Title: Dynamic-Hash-Table Based Public Auditing for Secure Cloud Storage**

**Author/Year: Mruga Gurjar, Parth Naik/2018**

**Description:**

Cloud storage is an increasingly popular application of cloud computing, which can provide on-demand outsourcing data services for both organizations and individuals. However, users may not fully trust the cloud service providers (CSPs) in that it is difficult to determine whether the CSPs meet their legal expectations for data security. Therefore, it is critical to develop efficient auditing techniques to strengthen data owners' trust and confidence in cloud storage. In this paper, we present a novel public auditing

scheme for secure cloud storage based on dynamic hashtable (DHT), which is a new two-dimensional data structure located at a third-party auditor (TPA) to record the data property information for dynamic auditing. Differing from the existing works, the proposed scheme migrates the authorized information from the CSP to the TPA, and thereby significantly reduces the computational cost and communication overhead. Meanwhile, exploiting the structural advantages of the DHT, our scheme can also achieve higher updating efficiency than the state-of-the-art schemes. In addition, we extend our scheme to support privacy preservation by combining the homomorphic authenticator based on the public key with the random masking generated by the TPA, and achieve batch auditing by employing the aggregate BLS signature technique. We formally prove the security of the proposed scheme, and evaluate the auditing performance by detailed experiments and comparisons with the existing ones. The results demonstrate that the proposed scheme can effectively achieve secure auditing for cloud storage, and outperforms the previous schemes in computation complexity, storage costs and communication overhead.

## **OPEN PROBLEMS IN EXISTING SYSTEM**

While Cloud Computing makes these advantages more appealing than ever, it also brings new and challenging security threats towards users' outsourced data. Since cloud service providers (CSP) are separate administrative entities, data outsourcing is actually relinquishing user's ultimate control over the fate of their data. As a result, the correctness of the data in the cloud is being put at risk due to the following reasons. Although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, they are still facing the broad range of both internal and

external threats for data integrity. There do exist various motivations for CSP to behave unfaithfully towards the cloud users regarding their outsourced data status. For examples, CSP might reclaim storage for monetary reasons by discarding data that has not been or is rarely accessed, or even hide data loss incidents to maintain a reputation. In short, although outsourcing data to the cloud is economically attractive for long-term large-scale storage, it does not immediately offer any guarantee on data integrity and availability. This problem, if not properly addressed, may impede the success of cloud architecture.

As users no longer physically possess the storage of their data, traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted. In particular, simply downloading all the data for its integrity verification is not a practical solution due to the expensiveness in I/O and transmission cost across the network. Besides, it is often insufficient to detect the data corruption only when accessing the data, as it does not give users correctness assurance for those unaccessed data and might be too late to recover the data loss or damage. Considering the large size of the outsourced data and the user's constrained resource capability, the tasks of auditing the data correctness in a cloud environment can be formidable and expensive for the cloud users. Moreover, the overhead of using cloud storage should be minimized as much as possible, such that a user does not need to perform too many operations to use the data (in addition to retrieving the data). In particular, users may not want to go through the complexity in verifying the data integrity. Besides, there may be more than one user accessing the same cloud storage, say in an enterprise setting. For easier management, it is desirable that cloud only entertains verification request from a single designated party.

## **DISADVANTAGES**

### **Abuse and Nefarious Use of Cloud Computing:**

IaaS providers offer their customers the illusion of unlimited compute, network, and storage capacity often coupled with a 'frictionless' registration process where anyone with a valid credit card can register and immediately begin using cloud services. Some providers even offer free limited trial periods. By abusing the relative anonymity behind these registration and usage models, spammers, malicious code authors, and other criminals have been able to conduct their activities with relative impunity. PaaS providers have traditionally suffered most from this kind of attacks; however, recent evidence shows that hackers have begun to target IaaS vendors as well. Future areas of concern include password and key cracking, DDOS, launching dynamic attack points, hosting malicious data, botnet command and control, building rainbow tables, and CAPTCHA solving farms.

### **Insecure Interfaces and APIs:**

Cloud computing providers expose a set of software interfaces or APIs that customers use to manage and interact with cloud services. Provisioning, management, orchestration, and monitoring are all performed using these interfaces. The security and availability of general cloud services is dependent upon the security of these basic APIs. This introduces the complexity of the new layered API; it also increases risk, as organizations may be required to relinquish their credentials to third parties in order to enable their agency.

### **Malicious Insiders:**

The threat of a malicious insider is well-known to most organizations. This threat is amplified for consumers of cloud services by the convergence of IT

services and customers under a single management domain, combined with a general lack of transparency into provider process and procedure

### **Shared Technology Issues:**

IaaS vendors deliver their services in a scalable way by sharing infrastructure. Often, the underlying components that make up this infrastructure were not designed to offer strong isolation properties for a multi-tenant architecture.

### **Data Loss or Leakage:**

There are many ways to compromise data. Deletion or alteration of records without a backup of the original content is an obvious example

### **Account or Service Hijacking:**

Account or service hijacking is not new. Attack methods such as phishing, fraud, and exploitation of software vulnerabilities still achieve results

## **CHAPTER3**

### **AIMANDSCOPEOFTHEPRESENTINVESTIGATION**

#### **AIM**

The aim of this project is to enhance the security and fault tolerance of transactions in cloud banking by integrating blockchain technology. The project will focus on developing a secure and efficient framework that leverages blockchain to ensure the integrity, confidentiality, and availability of financial transactions conducted through cloud banking platforms.

#### **SCOPE**

- Investigate the current challenges and vulnerabilities in cloud banking systems related to transaction security and fault tolerance.
- Design and develop a blockchain-based framework for cloud banking that addresses these challenges, focusing on secure transaction processing and fault tolerance mechanisms.
- Implement the proposed framework and conduct thorough testing to evaluate its performance, security, and fault tolerance capabilities.
- Compare the proposed framework with existing approaches and analyze its advantages in terms of security, efficiency, and scalability.
- Provide guidelines and recommendations for the adoption and integration of blockchain technology in cloud banking systems to enhance transaction security and fault tolerance.

## **RISK ANALYSIS OF THE PROJECT**

The software requirement specification gives the system specification in which process requirements are represented in an easily understandable way. Thus it contains all the inputs required, processes in the system and outputs produced by the system.

Software Requirements Specification plays an important role in creating quality software solutions. Specification is basically a representation process. Requirements are represented in a manner that ultimately leads to successful software implementation.

Requirements may be specified in a variety of ways. However there are some guidelines worth following

- Representation format and contents should be relevant to the problem.
- Information contained within the specifications should be nested.

Requirement analysis enables the system engineer to specify software function and perform, indicate software's interface with the other system elements, and establish constraints that software must meet. Requirement analysis allows the analyst to refine the software allocation and build models of the data, functional and behavioral domains that will be treated by software.

The first step is to understand the user's requirement within the framework of the organization's objectives and the environment in which the system is

installed. Considerations are given to the user to carry on with the work within the organization's specified objectives.

Using swings in java we will develop the proposed system. The proposed application can be implemented by taking minimum of three systems into consideration. The server is implemented in one system, TPA is implemented in another system, and client can be implemented from any system. It can be implemented on any operating system like windows or linux. The client system will store data like files, images on to server through TPA. The TPA will store the metadata information of file on TPA, whereas server will store files as well as metadata information about the files. Whenever the client asks for the verification of files on cloud, the TPA will check for the data integrity on the server. This application demands minimum three systems should be connected within a network.

## **FEASIBILITY STUDY**

The feasibility of the project is analyzed in this phase, and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis, the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

## **ECONOMICAL FEASIBILITY**

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour

into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

### **TECHNICAL FEASIBILITY**

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

### **SOCIAL FEASIBILITY**

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

# SOFTWARE REQUIREMENTS SPECIFICATION DOCUMENT

## HARDWARE AND SOFTWARE REQUIREMENTS

- Server and Client Side Technology : AWT and Swings.
- Database : MySQL
- Operating System : Windows 95/98/2000/XP
- Processor : Pentium 4 processor
- RAM : 1GB RAM
- Hard Disk : 80GB Hard Disk Space

## **CHAPTER4**

### **EXPERIMENTALORMATERIALSANDMETHODS; ALGORITHMS USED**

#### **PROPOSEDSYSTEM**

Theproposedsystemcanbesummarizedasthefollowingthreeaspects:

1. We motivate the public auditing system of data storage security in Cloud Computing and provide a privacy-preserving auditing protocol, i.e., our scheme supports an external auditor to audit user's outsourced data in the cloud without learning knowledge on the data content.

2. To the best of our knowledge, our scheme is the first to support scalable and efficient public auditing in the Cloud Computing. In particular, our scheme achieves batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the TPA.

2. We prove the security and justify the performance of our proposed schemes through concrete experiments and comparisons with the state-of-the-art.

#### **ADVANTAGES**

- Novelautomaticandenforceableloggingmechanisminthecloud.
- Proposed architecture is platform independent and highly

decentralized, in that it does not require any dedicated authentication or storage system in place.

- Provide a certain degree of usage control for the protected data after these are delivered to the receiver
- The results demonstrate the efficiency, scalability, and granularity of our approach. We also provide a detailed security analysis and discuss the reliability and strength of our architecture.

### **MODULE DESCRIPTION:**

The system is proposed to have the following modules:

- AdminModule
- TPA module
- UserModule
- BlockVerificationModule
- BlockInsertionModule
- BlockDeletion

### **ADMINMODULE**

Admin is allowed to check which user registered and which data is stored in the cloud space area .

### **TPA MODULE**

TPA check that data is modified or not if modified that information send to user.

## **USERMODULE**

User can register and he can login with his user id and password and he can upload the data to cloud space area.

## **BLOCKVERIFICATIONMODULE**

User can check that the uploaded file is modified by any one or not (like server area).

## **BLOCKINSERTIONMODULE**

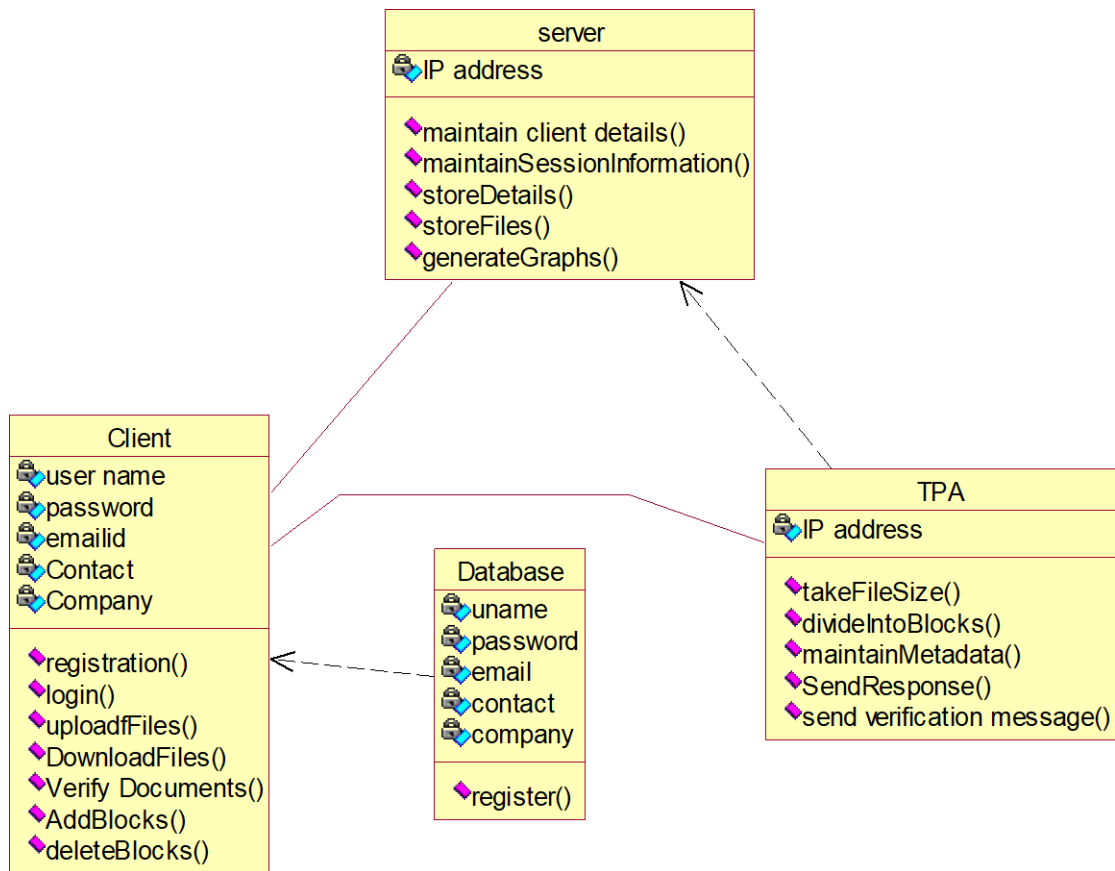
In the block insertion module user can insert the new block.

## **BLOCKDELETIONMODULE**

In the Block Deletion Module user can delete the Block.

## **CLASS DIAGRAM AUDITING FOR SECURED DATA STORAGE IN CLOUD**

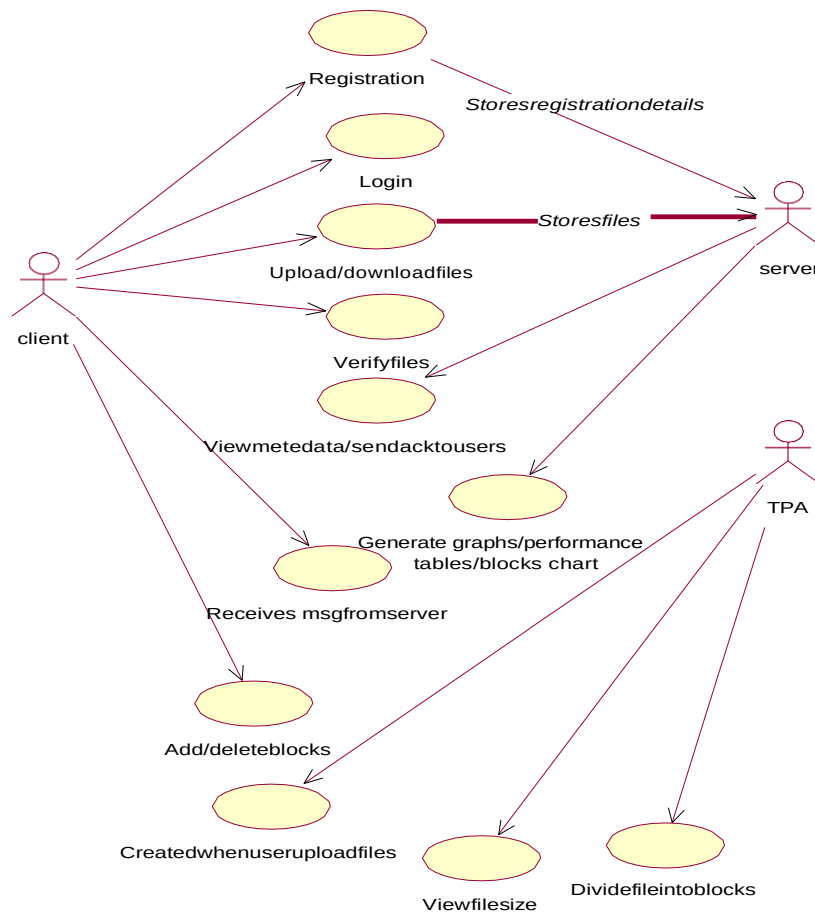
This class diagram contains four classes that are Server, TPA, Client and Database. Server will perform operations like it maintains client details & session information, stores details & files and generate graphs. Client will perform operations like registration, login, upload files, download files, verify documents, add blocks, delete blocks. TPA will perform operations like take file size, divide file into blocks, maintain metadata information, send response and verification message. And this diagram shows the relationship between these classes.



**FIG4.1.1CLASSDIAGRAM**

## USECASEDIAGRAM:

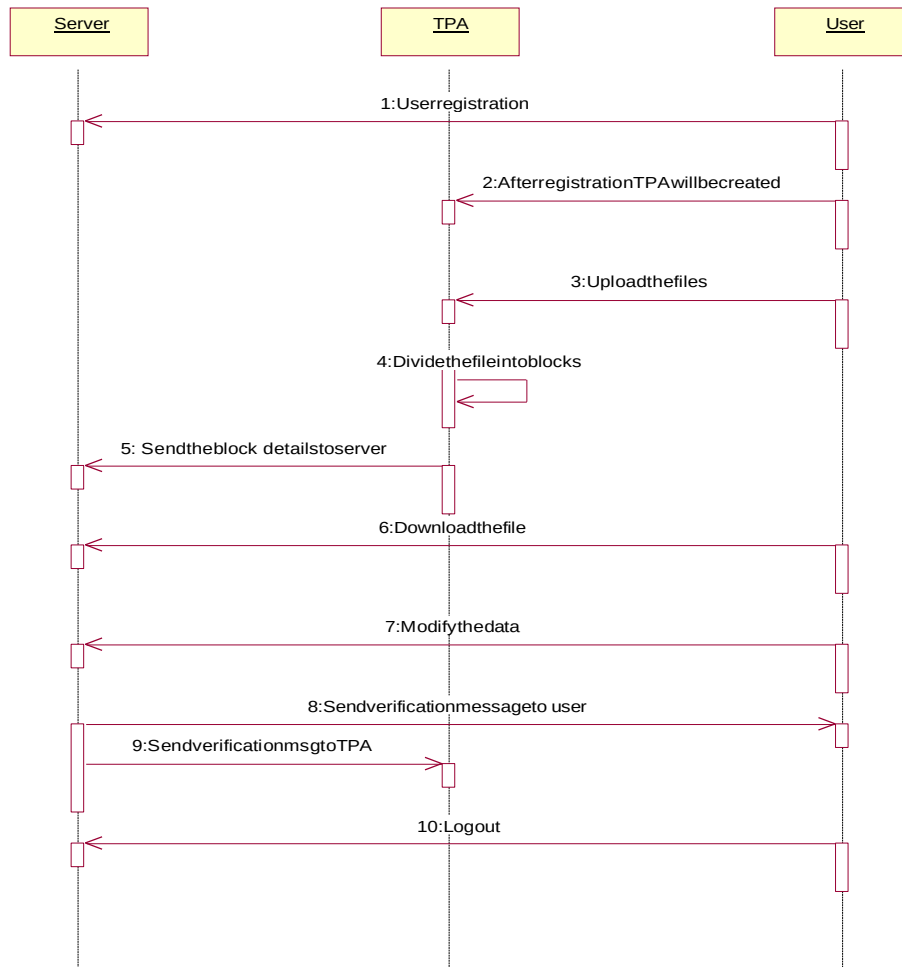
This use case diagram contains three actors that are Server, TPA, Client and. Server will perform operations like it maintains client details & session information, stores details & files and generate graphs. Client will perform operations like registration, login, upload files, download files, verify documents,addblocks,deleteblocks.TPAwillperformoperationsliketake file size, divide file into blocks, maintain metadata information, send response and verification message. And this diagram shows the use cases of each actor and relationship between this actors and use cases.



**FIG4.1.2USECASEDIAGRAM**

## SEQUENCEDIAGRAM:

This sequence diagram contains three objects that are Server, TPA, Client and. Server will perform operations like it maintains client details & session information stores details & files and generate graphs. Client will perform operations like registration, login, upload files, download files, verify documents, add blocks, delete blocks. TPA will perform operations like take file size, divide file into blocks, maintain metadata information, send response and verification message. And this diagram shows the sequence of actions performed between these objects.

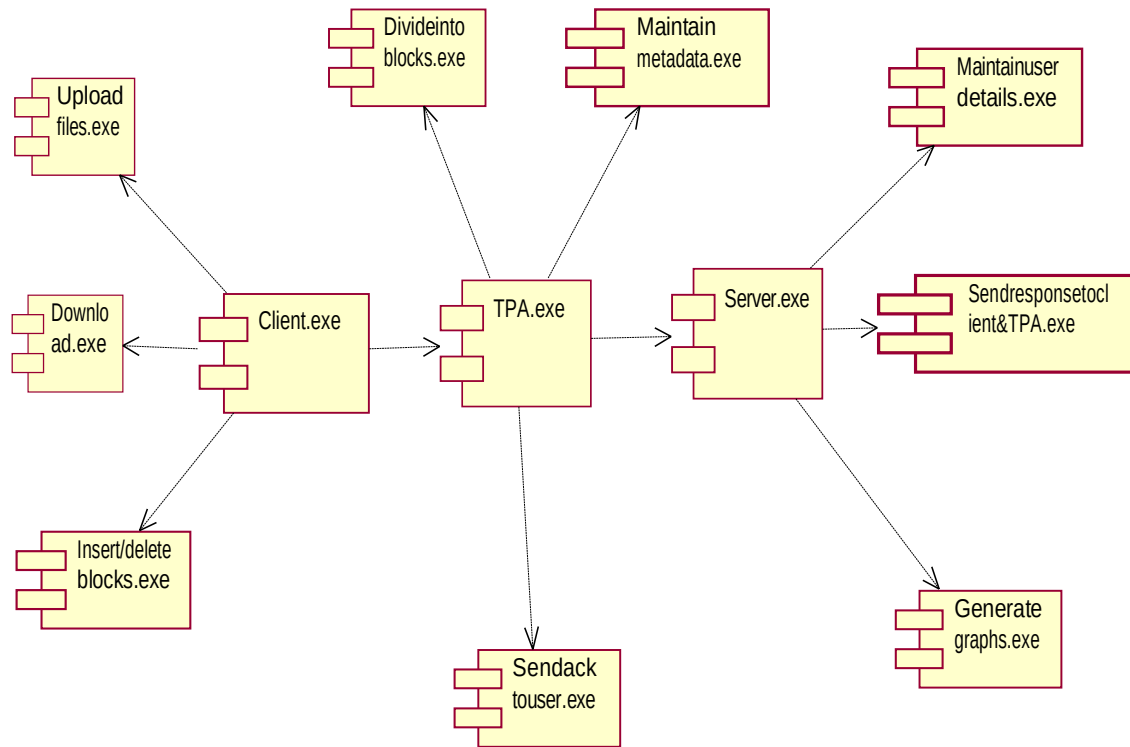


**FIG4.1.3 SEQUENCE DIAGRAM**

### COMPONENT DIAGRAM:

This component diagram contains three components that are Server, TPA, Client and. Server will perform operations like it maintains client details & session information stores details & files and generate graphs. Client will perform operations like registration, login, upload files, download files, verify documents, add blocks, delete blocks. TPA will perform operations like take filesize, divide file into blocks, maintain metadata information, send

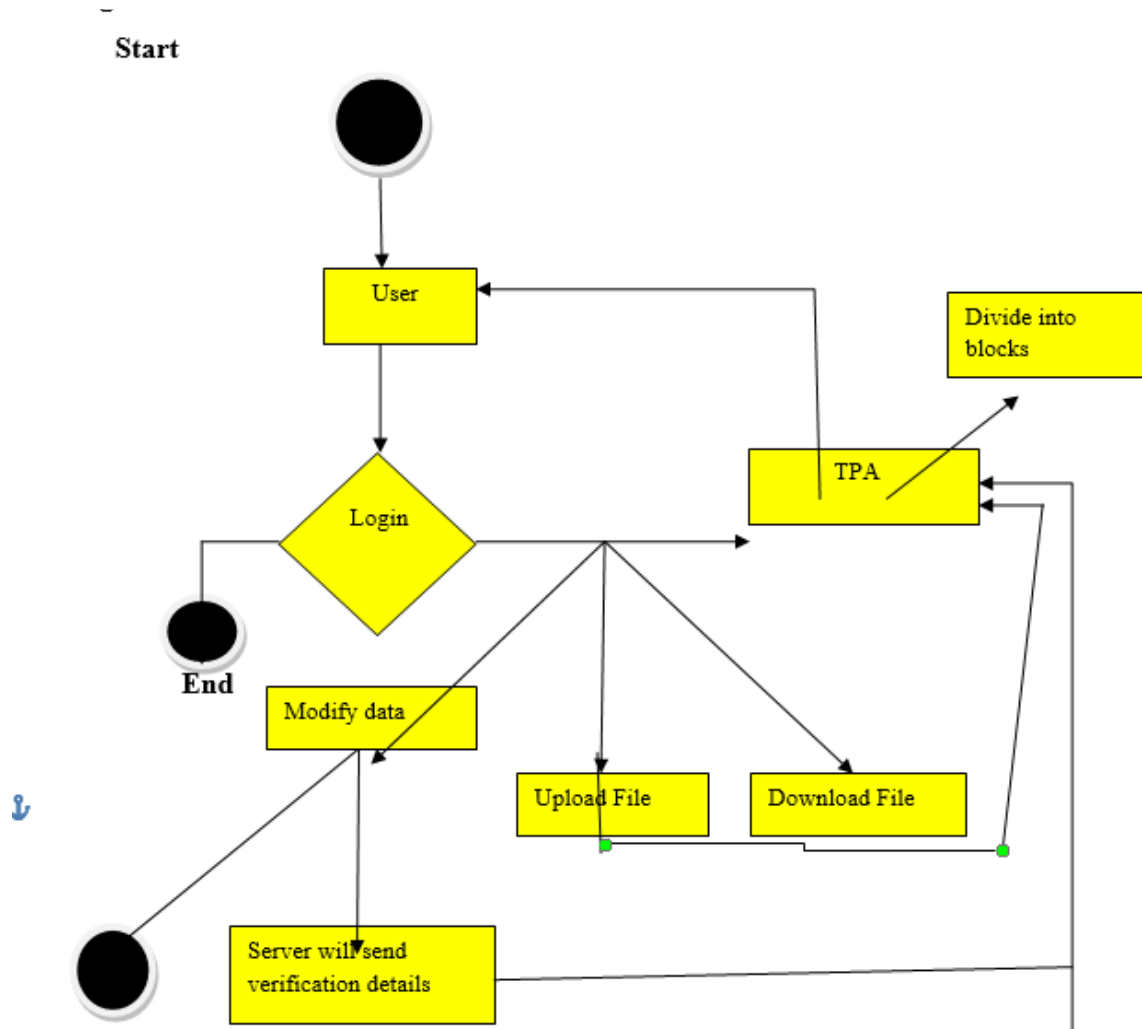
response and verification message. And this diagram shows the actions performed by these components.



**FIG4.1.4 COMPONENT DIAGRAM**

#### **ACTIVITY DIAGRAM:**

This activity diagram contains three activities that are Server, TPA, Client and. This diagram shows the flow of control between these activities.



**FIG4.1.5ACTIVITYDIAGRAM**

## UNIFIEDMODELINGLANGUAGE

The Unified Modelling Language allows the software engineer to express an analysis model using the modelling notation that is governed by a set of syntactic semantic and pragmatic rules.

A UML system is represented using five different views that describe the system from distinctly different perspectives. Each view is defined by a set of diagram, which is as follows.

- **UserModel View**

- This view represents the system from the user's perspective.
- The analysis representation describes a usage scenario from the end-users perspective.

- **Structural model view**

- In this model the data and functionality are arrived from inside the system.
- This model view models the static structures.

- **Behavioral Model View**

It represents the dynamic of behavioral aspects of the system, depicting the interactions of collection between various structural elements described in the user model and structural model view.

- **Implementation Model View**

In this the structural and behavioral aspects of the system are represented as they are to be built.

- **Environmental Model View**

In this the structural and behavioral aspects of the environment in which the system is to be implemented are represented.

UML is specifically constructed through two different domains they are:

- UML Analysis modeling, this focuses on the user model and structural model views of the system.

- UML design modeling, which focuses on the behavioral modeling, implementation modeling and environmental model views.

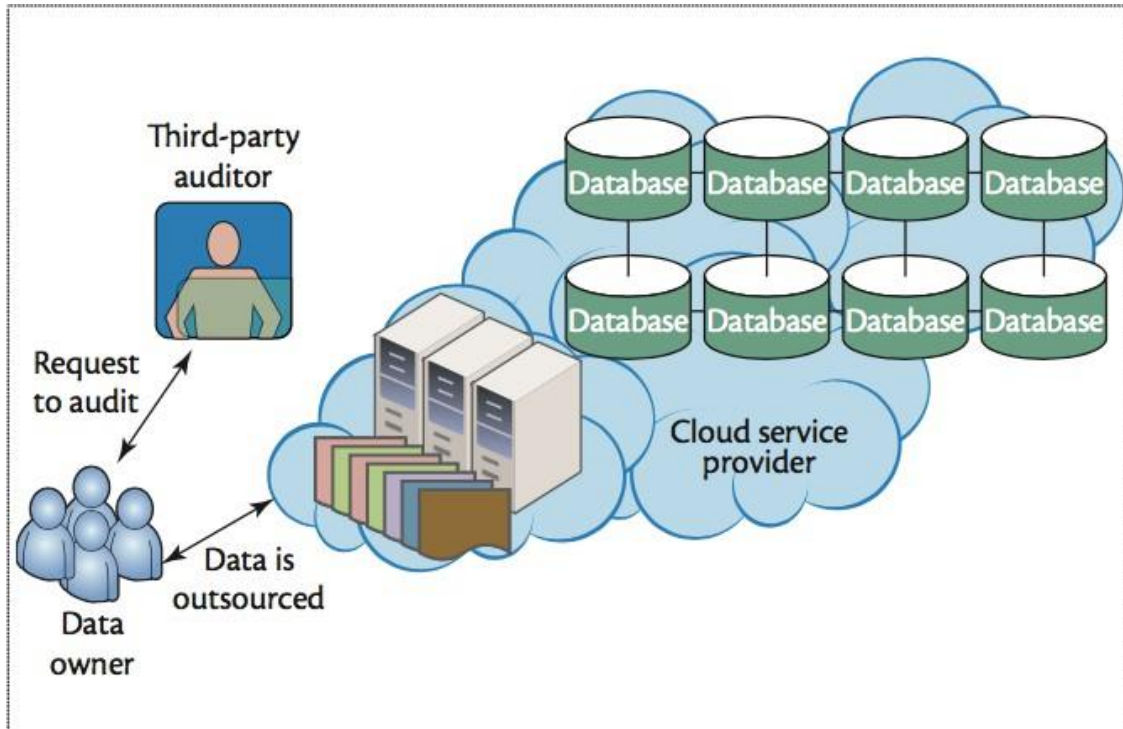
Use case Diagrams represent the functionality of the system from a user's point of view. Use cases are used during requirements elicitation and analysis to represent the functionality of the system. Use cases focus on the behavior of the system from external point of view.

Actors are external entities that interact with the system. Examples of actors include users like administrator, bank customer ...etc., or another system like central database.

## **ARCHITECTURE/OVERALL DESIGN OF PROPOSED SYSTEM**

### **SYSTEM ARCHITECTURE**

Describing the overall features of the software is concerned with defining the requirements and establishing the high level of the system. During architectural design, the various web pages and their interconnections are identified and designed. The major software components are identified and decomposed into processing modules and conceptual data structures and the interconnections among the modules are identified. The following modules are identified in the proposed system.



**FIG4.2SYSTEMARCHITECTUREDIAGRAM**

## **DESCRIPTION OF SOFTWARE FOR IMPLEMENTATION AND TESTING PLAN OF THE PROPOSED MODEL/SYSTEM**

The purpose of the Software Requirement Specification is to produce the specification of the analysis task and also to establish complete information about the requirement, behavior and also the other constraint like functional performance and so on. The main aim of the Software Requirement Specification is to completely specify the technical requirements for the software product in a concise and in unambiguous manner.

## VISUALSTUDIO

In this project the Microsoft visual studio is used as an IDE. Visual Studio Code combines the simplicity of a source code editor with powerful developer tooling, like Intelli Sense code completion and debugging. First and foremost, it is an editor that gets out of our way. The delightfully frictionless edit-build-debug cycle means less time fiddling with our environment, and more time executing on our ideas. Visual Studio Code supports macOS, Linux, and Windows - so we can hit the ground running, no matter the platform. At its heart, Visual Studio Code features a lightning fast source code editor, perfect for day-to-day use. With support for hundreds of languages, VS Code helps us be instantly productive with syntax highlighting, bracket-matching, auto-indentation, box-selection, snippets, and more. Intuitive keyboard shortcuts, easy customization and community-contributed keyboard shortcut mappings let us navigate our code with ease. For serious coding, we'll often benefit from tools with more code understanding than just blocks of text. Visual Studio Code includes built-in support for IntelliSense code completion, rich semantic code understanding and navigation, and code refactoring. And when the coding gets tough, the tough get debugging. Debugging is often the one feature that developers miss most in a leaner coding experience, so we made it happen. Visual Studio Code includes an interactive debugger, so we can step through source code, inspect variables, view call stacks, and execute commands in the console. VS Code also integrates with build and scripting tools to perform common tasks making everyday workflows faster. VS Code has support for Git so we can work with source control without leaving the editor including viewing pending changes and diffs. Visual Studio Code includes a

public extensibility model that lets developers build and use extensions, and richly customize their edit-build-debug experience.

## **JAVA**

Java is one of the world's most important and widely used computer languages, and it has held this distinction for many years. Unlike some other computer languages whose influence has waned with passage of time, while Java's has grown.

## **APPLICATION OF JAVA**

Java is widely used in every corner of world and of human life. Java is not only used in softwares but is also widely used in designing hardware controlling software components. There are more than 930 million JRE downloads each year and 3 billion mobile phones run java.

Following are some other usage of Java:

1. Developing Desktop Applications
2. Web Applications like LinkedIn.com, Snapdeal.com etc
3. Mobile Operating System like Android
4. Embedded Systems
5. Robotics and games etc.

## **FEATURES OF JAVA**

The prime reason behind creation of Java was to bring portability and security feature into a computer language. Besides these two major features,

there were many other features that played an important role in moulding out the final form of this outstanding language. Those features are;

### **1) Simple**

Java is easy to learn and its syntax is quite simple, clean and easy to understand. The confusing and ambiguous concepts of C++ are either left out in Java or they have been re-implemented in a cleaner way.

*Eg:* Pointers and Operator Overloading are not there in java but were an important part of C++.

### **2) Object Oriented**

In java everything is Object which has some data and behaviour. Java can be easily extended as it is based on Object Model.

### **3) Robust**

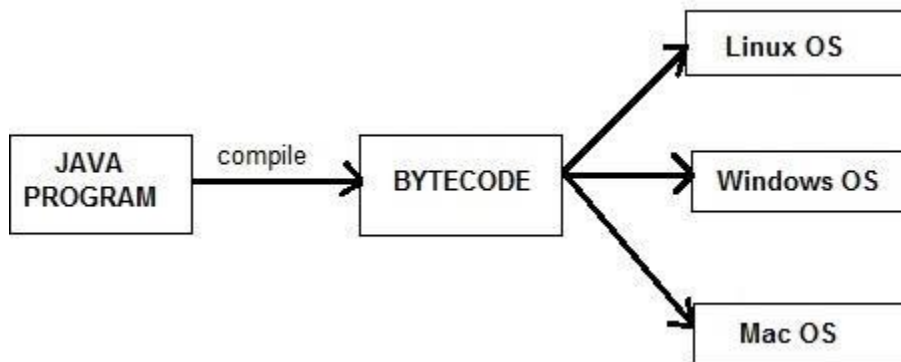
Java makes an effort to eliminate error prone codes by emphasizing mainly on compile time error checking and runtime checking. But the main areas which Java improved were Memory Management and mishandled Exceptions by introducing automatic Garbage Collector and Exception Handling.

### **4) Platform Independent**

Unlike other programming languages such as C, C++ etc. which are compiled into platform specific machines. Java is guaranteed to be write-once, run-anywhere language.

On compilation Java program is compiled into byte code. This byte code is platform independent and can be run on any machine, plus this byte code

format also provide security. Any machine with Java Runtime Environment can run Java Programs.



## 5) Secure

When it comes to security, Java is always the first choice. With java secure features it is able to develop virus-free, tamper-free system. Java program always runs in Java runtime environment with almost null interaction with system OS, hence it is more secure.

## 6) Multi-Threading

Java multithreading feature makes it possible to write program that can do many tasks simultaneously. Benefit of multithreading is that it utilizes same memory and other resources to execute multiple threads at the same time, like While typing, grammatical errors are checked along.

## 7) Architectural Neutral

Compiler generates byte codes, which have nothing to do with a particular computer architecture, hence a Java program is easy to interpret on any machine.

## **8) Portable**

Java Byte code can be carried to any platform. No implementation dependent features. Everything related to storage is predefined, example: size of primitive data types

## **10)High Performance**

Java is an interpreted language, so it will never be as fast as a compiled language like C or C++. But, Java enables high performance with the use of just-in-time compiler.

# **SYSTEM STUDY**

## **TESTING PROCESS:**

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub-assemblies, assemblies and/or a finished product. It is the process of exercising software with the intent of ensuring that the software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

## **TYPES OF TESTS:**

### **UNIT TESTING:**

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program input produces valid outputs. All decision branches and internal code flows should be validated. It is the testing of individual software units of the application. It is done after the completion of an individual unit before integration. This is a structural

testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

### **INTEGRATION TESTING :**

Integration tests are designed to test integrated software components to determine if they actually run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration tests demonstrate that although the components were individually satisfactory, as shown by successfully unit testing, the combination of components is incorrect and consistent. Integration testing is specifically aimed at exposing the problems that arise from the combination of components.

### **FUNCTIONAL TESTING :**

Functional tests provide systematic demonstration that functions tested are available as specified by the business and technical requirements, system documentation and user manuals.

Functional testing is centered on the following items:

Valid Input is used to identified classes of valid input must be accepted.  
Invalid Input is used to identified classes of invalid input must be rejected.  
Functions is used to identified functions must be exercised. Output is used to identify classes of application outputs.

Systems/Procedures is used to interfacing systems or procedures must be invoked. Organization and preparation of functional tests is focused on

requirements, key functions, or special test cases. In addition, systematic coverage pertaining to identify Business process flows; data fields, predefined processes, and successive Processes must be considered for testing. Before functional testing is complete, additional tests are identified and the effective value of current tests is determined.

### **SYSTEM TESTING:**

System testing ensures that the entire integrated software system meets requirements. It tests a configuration to ensure known and predictable results. An example of system testing is the configuration oriented system integration test. System testing is based on process descriptions and flows, emphasizing pre-Driven process links and integration points.

### **WHITE BOX TESTING:**

White Box Testing is a testing in which the software tester has knowledge of the inner workings, structure and language of the software, or at least its purpose. It is used to test areas that cannot be reached from a black box level.

### **BLACK BOX TESTING:**

Black Box Testing is testing the software without any knowledge of the inner workings, structure or language of the module being tested. Black box tests, as most other kinds of tests, must be written from a definitive source document, such as specification or requirements document, such as specification or requirement document. It is a testing in which the software under test is treated, as a black box. you cannot "see" into it. The test

provides inputs and responds to outputs without considering how the software works.

## **TEST STRATEGY AND APPROACH**

Field testing will be performed manually and functional tests will be written in detail.

1. All field entries must work properly.
2. Pages must be activated from the identified link.
3. The entry screen, messages and responses must not be delayed.

Features to be tested.

4. Verify that the entries are of the correct format. No duplicate entries should be allowed.
5. All links should take the user to the correct page.

## **INTEGRATION TESTING:**

Software integration testing is the incremental integration testing of two or more integrated software components on a single platform to produce failures caused by interface defects. The task of the integration test is to check that components or software applications.

## **ACCEPTANCE TESTING:**

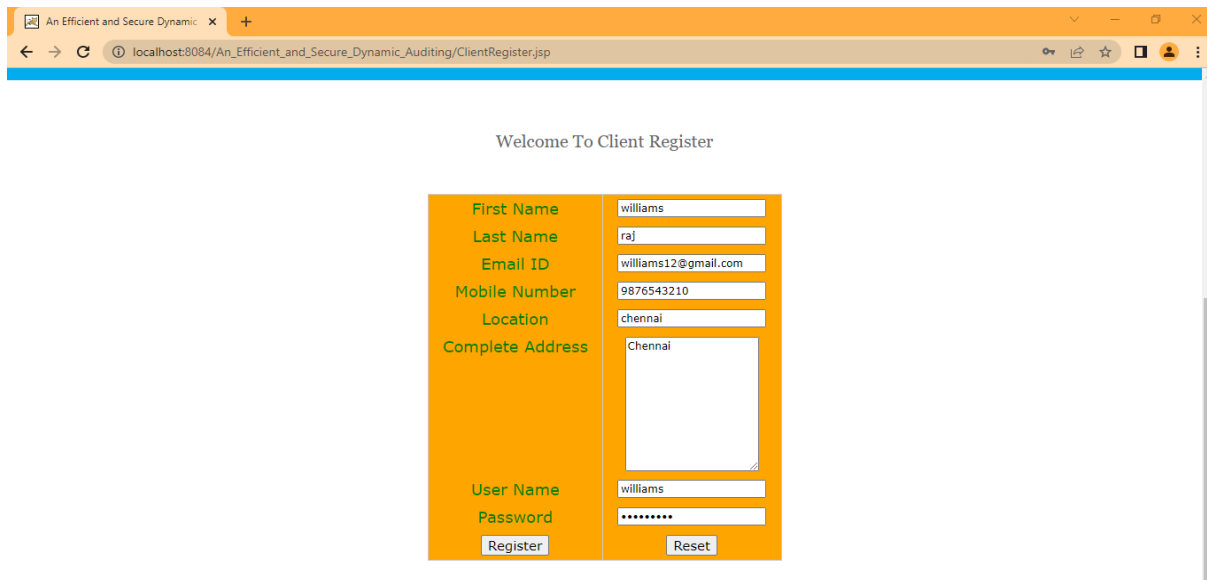
User Acceptance Testing is a critical phase of any project and requires significant participation by the end user. It also ensures that the system meets the functional requirements.

## CHAPTER 5

### RESULTSANDDISCUSSIONS

#### RESULTS

To begin with, we can split our modules of implementation that is done. The login page can be shown in the below figure.



The screenshot shows a web browser window with the address bar displaying 'localhost:8084/An\_Efficient\_and\_Secure\_Dynamic\_Auditing/ClientRegister.jsp'. The page content includes a heading 'Welcome To Client Register' and a registration form. The form has a yellow background and contains the following fields and labels:

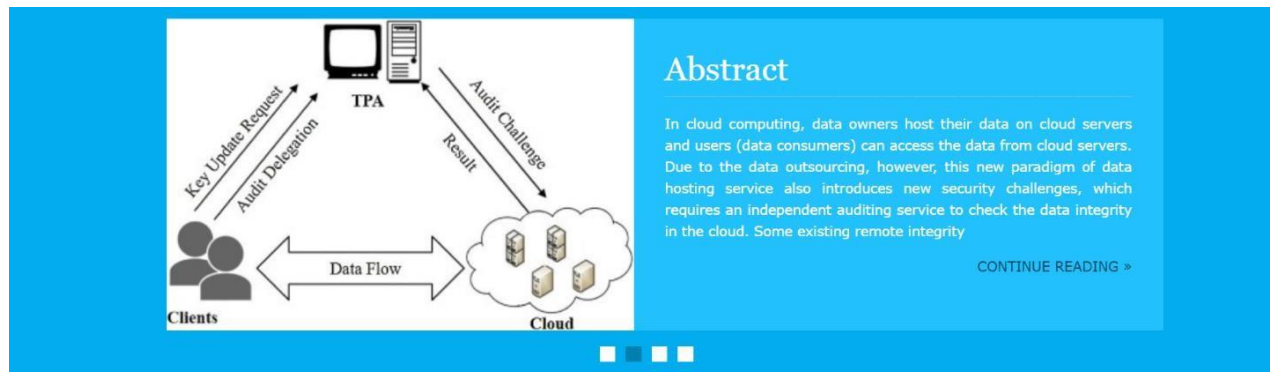
| Field Label      | Value                |
|------------------|----------------------|
| First Name       | williams             |
| Last Name        | raj                  |
| Email ID         | williams12@gmail.com |
| Mobile Number    | 9876543210           |
| Location         | chennai              |
| Complete Address | Chennai              |
| User Name        | williams             |
| Password         | *****                |

At the bottom of the form, there are two buttons: 'Register' and 'Reset'.

***Fig5.1 Loginpage***



**Fig5.2ClientRegistration**



Upload File Here

|                                       |                                                           |
|---------------------------------------|-----------------------------------------------------------|
| File ID                               | <input type="text" value="8"/>                            |
| Subject                               | <input type="text"/>                                      |
| Choose File                           | <input type="button" value="Choose File"/> No file chosen |
| <input type="button" value="Upload"/> |                                                           |

**Fig5.3UploadFile**



File Sending With Meta Key

| Blocks | Secrete Key          | Metadata Key | Status | Send                                |
|--------|----------------------|--------------|--------|-------------------------------------|
| Block1 | <input type="text"/> |              |        | <input type="button" value="Send"/> |

|                      |            |
|----------------------|------------|
| Each Block Size      | 10.6 Bytes |
| Total Size           | 53.0 Bytes |
| <a href="#">Back</a> |            |

**Fig5.4FileSendingMetaKey**



| Blocks | Secrete Key                             |
|--------|-----------------------------------------|
| Block1 | <input type="text" value="s1"/>         |
| Block2 | <input type="text" value="s2"/>         |
| Block3 | <input type="text" value="s3"/>         |
| Block4 | <input type="text" value="s4"/>         |
| Block5 | <input type="text" value="s5"/>         |
|        | <input type="button" value="Download"/> |

**Fig5.5SecretKey**

Welcome to Client Home :hup@gmail.com

## DOWNLOAD HISTORY

| FileName | Downloaded Date     |
|----------|---------------------|
| demo.txt | 2024-03-23 14:41:00 |

***Fig5.6DownloadHistory***

## **CHAPTER 6**

### **SUMMARY AND CONCLUSION**

#### **5.1 CONCLUSION:**

In this project, we propose a cloud auditing system for data storage security in Cloud Computing. We utilize the homomorphic linear authenticator and random masking to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users' fear of their outsourced data leakage. Considering TPA may concurrently handle multiple audit sessions from different users for their outsourced data files, we further extend our privacy preserving public auditing protocol into a multi-user setting, where the TPA can perform multiple auditing tasks in a batch manner for better efficiency. Extensive analysis shows that our schemes are provably secure and highly efficient.

## REFERENCES

- a. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Storage Security in Cloud Computing," Proc. IEEE INFOCOM '10, Mar. 2010.
- b. H. Mell and T. Grance, "Draft NIST Working Definition of Cloud Computing," <http://csrc.nist.gov/groups/SNS/cloudcomputing/index.html>, June 2009.
- c. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the Clouds: A Berkeley View of Cloud Computing," Technical Report UCB-EECS-2009-28, Univ. of California, Berkeley, Feb. 2009.
- d. M. Arrington, "Gmail Disaster: Reports of Mass Email Deletions," <http://www.techcrunch.com/2006/12/28/gmail-disasterreportsof-mass-email-deletions/>, 2006.
- e. P. Arston Cloud Security Alliance, "Top Threats to Cloud Computing," <http://www.cloudsecurityalliance.org>, 2010.
- f. R. Akimane, O. Markowitch, and Y. Roggeman, "Secure outsourcing of DNA sequences comparisons in a Grid environment," WSEAS Trans. Comput. Res., vol. 2, no. 2, pp. 262–269, Feb. 2007.

## APPENDIX

### A. SOURCECODE

```
<htmlxmlns="http://www.w3.org/1999/xhtml">

<head>

<title>Secureblockchainbankingwitherrorrecoveryprocess</title>

<metahttp-equiv="Content-Type"content="text/html;charset=iso-8859-1"/>

<linkrel="stylesheet"href="layout/styles/layout.css"type="text/css"/>

<scripttype="text/javascript"src="layout/scripts/jquery.min.js"></script>

<script
type="text/javascript"src="layout/scripts/jquery.slidepanel.setup.js"></script>

<!--HomepageOnlyScripts-->

<script
type="text/javascript"src="layout/scripts/jquery.cycl
e.min.js"></script>

<scripttype="text/javascript">

$(function){

    $('#featured_slide').after('<divid="fsn"><ulid="fs_pagination">').cycle({

        timeout: 5000,

        fx:'fade',

        pager:'#fs_pagination',

        pause: 1,

        pauseOnPagerHover:0

    });
```

```

});

</script>

<!--EndHomepageOnlyScripts-->

</head>

<body>

<divclass="wrappercol1">

    <divid="header">

        <divid="logo">

            <h2><a href="index.html">Secureblockchainbankingwith
</a><span>errorrecoveryprocess</span><h2>

            <p></p>

        </div>

        <divid="topnav">

            <ul>

                <li><a href="index.html">Home</a></li>

                <liclass="active"><a href="Client.jsp">Client</a></li>

                <li><a href="TPALogin.jsp">TPA</a></li>

                <li><a href="CloudServer.jsp">CloudServer</a></li>

            </ul>

        </div>

        <brclass="clear"/>

    </div>

```

</div>

<divclass="wrappercol2">

<divid="featured\_slide">

<divclass="featured\_box"><ahref="#"></a>

<divclass="floater">

<h3>Secureblockchainbankingwitherrorrecoveryprocess</h3>

</div>

</div>

<divclass="featured\_box"><ahref="#"></a>

<divclass="floater">

<h2>Abstract</h2>

<p align="justify">Incloudcomputing,dataownershosttheirdataon cloud  
servers and users (data consumers) can access the data

fromcloudservers.Duetothedataoutsourcing,however,thisnewparadigm of data  
hosting service also introduces new security

challenges,whichrequiresanindependentauditingstoservicecheckthedata integrity  
in the cloud. Some existing remote integrity</p>

<p class="readmore"><a href="https://sci-  
hub.tw/10.1109/tpds.2012.278">ContinueReading&raquo;</a></p>

</div>

</div>

<divclass="featured\_box"><ahref="#"><imgsrc="images\demo\existing  
picture.jpg" alt="" /></a>

<divclass="floater">

## <h2>ExistingSystem</h2>

<p align="justify">To solvethedataprivacyproblem,existingmethodis to generate an encrypted proof with the challenge stamp by using the Bilinearity property of the bilinear pairing, such that the auditor cannot decryptitbutcanverifythecorrectnessoftheproof.Withoutusingthemark technique, this method does not require any trusted organizer during the batch auditing for multiple clouds. Therefore, existing method can greatly reduce the computing loads of the auditor by moving it to the cloud server.</p>

<p class="readmore"><a href="https://sci-hub.tw/10.1109/tpds.2012.278">ContinueReading&raquo;</a></p>

</div>

</div>

<divclass="featured\_box"><a href="#"></a>

<divclass="floater">

## <h2>ProposedSystem</h2>

<p align="justify">To improve the draw backs of existing system a modifieddynamicauditingprotocolisintroduced,Thisprotocolcontains 1.Time stamp value to verify the validity of data 2.Index table for dynamic owneraswellasdata.Thissystemincludes4modules1.Multicloudstorages 2. Modifieddynamicauditing3.DataIntegrityandThirdPartyAuditor4. Dynamic auditing</p>

<p class="readmore"><a href="https://sci-hub.tw/10.1109/tpds.2012.278">ContinueReading&raquo;</a></p>

</div>

</div>

</div>

</div>

</div>

<divclass="wrappercol3">

<divid="homecontent">

<divclass="center">

<h1>WelcomeToClientLogin</h1>

<formname="login"action="ClientLogin.jsp"method="post">

<tablebgcolor="orange"style="margin-top:50px;width:300px;"  
align="center">

<tr>

<td><fontsize="4"color="green"style="">UserEmail</td>

<td><inputtype="text"name="uname"required></input></td>

</tr>

<tr>

<td><fontsize="4"color="green"style="">Password</td>

<td><inputtype="password"name="password"required></input></td>

</tr>

```

        <tr>

            <td><input type="Submit" value="Login" style="font-size:
15px;"></input></td>

            <td><input type="Reset" style="font-size:15px;"></input></td>

        </tr>

```

```

    </form>

```

```

</table>

```

```

        <tr><td><a href="ClientRegister.jsp">Click Here to
Register</a></td></tr><br></br>

```

```

        <!--<tr><td><a href="forgot.jsp" method="post"><font
color="red">Forgot Password?</a></td></tr> -->

```

```

    </div>

```

```

    <br class="clear"/>

```

```

</div>

```

```

</div>

```

```

<div class="wrapper col4">

```

```

    <div id="footer">

```

```

    </div>

```

```

    <br class="clear"/>

```

```

</div>

```

```

</div>

</body>

</html>Clien

tPage

<htmlxmlns="http://www.w3.org/1999/xhtml">

<head>

<title>Secureblockchainbankingwitherrorrecoveryprocess</title>

<metahttp-equiv="Content-Type"content="text/html;charset=iso-8859-1"/>

<linkrel="stylesheet"href="layout/styles/layout.css"type="text/css"/>

<scripttype="text/javascript"src="layout/scripts/jquery.min.js"></script>

<script
type="text/javascript"src="layout/scripts/jquery.slidepanel.setup.js"></script>

<!--HomepageOnlyScripts-->

<script
type="text/javascript"src="layout/scripts/jquery.cycl
e.min.js"></script>

<scripttype="text/javascript">

$(function){

    $('#featured_slide').after('<divid="fsn"><ulid="fs_pagination">').cycle({

        timeout: 5000,

        fx:'fade',

        pager:'#fs_pagination',

        pause: 1,

        pauseOnPagerHover:0

```

```

    });

});

</script>

<!--EndHomepageOnlyScripts-->

</head>

<body>

<divclass="wrappercol1">

    <divid="header">

        <divid="logo">

            <h2><a href="index.html">Secureblockchainbankingwith</a><span> error
recovery process</span></h2>

            <p></p>

        </div>

        <divid="topnav">

            <ul>

                <li><a href="index.html">Home</a></li>

                <li><a href="Client.jsp">Client</a></li>

                <liclass="active"><a href="TPALogin.jsp">TPA</a></li>

                <li><a href="CloudServer.jsp">CloudServer</a></li>

            </ul>

        </div>

```

```

        <brclass="clear"/>

    </div>

</div>

<divclass="wrappercol2">

    <divid="featured_slide">

        <divclass="featured_box"><ahref="#"></a>

        <divclass="floater">

            <h3>Secureblockchainbankingwitherrorrecoveryprocess</h3>

        </div>

    </div>

    <divclass="featured_box"><ahref="#"></a>

    <divclass="floater">

        <h2>Abstract</h2>

        <palign="justify">Incloudcomputing,dataownershosttheirdataon cloud
servers and users (data consumers) can access the data
fromcloudservers.Duetothedataoutsourcing,however,thisnewparadigm of data
hosting service also introduces new security
challenges,whichrequiresanindependentauditing servicetocheckthedata integrity
in the cloud. Some existing remote integrity</p>

        <p class="readmore"><a href="https://sci-
hub.tw/10.1109/tpds.2012.278">ContinueReading&raquo;</a></p>

    </div>

```

</div>

<div class="featured\_box"><a href="#"></a>

<div class="floater">

<h2>Existing System</h2>

<p align="justify">To solve the data privacy problem, existing method is to generate an encrypted proof with the challenge stamp by using the Bilinearity property of the bilinear pairing, such that the auditor cannot decrypt it but can verify the correctness of the proof. Without using the mask technique, this method does not require any trusted organizer during the batch auditing for multiple clouds. Therefore, existing method can greatly reduce the computing loads of the auditor by moving it to the cloud server.</p>

<p class="readmore"><a href="https://sci-hub.tw/10.1109/tpds.2012.278">Continue Reading</a></p>

</div>

</div>

<div class="featured\_box"><a href="#"></a>

<div class="floater">

<h2>Proposed System</h2>

<p align="justify">To improve the drawbacks of existing system a modified dynamic auditing protocol is introduced. This protocol contains  
1. Time stamp value to verify the validity of data  
2. Index table for dynamic owner as well as data. This system includes 4 modules  
1. Multicloud storage  
2. Modified dynamic auditing  
3. Data Integrity and Third Party Auditor  
4. Dynamic auditing.</p>

```
<p class="readmore"><a href="https://sci-
hub.tw/10.1109/tpds.2012.278">ContinueReading&raquo;</a></p>
```

```
</div>
```

```
</div>
```

```
</div>
```

```
</div>
```

```
</div>
```

```
<divclass="wrappercol3">
```

```
<divid="homecontent">
```

```
<divclass="center">
```

```
<divclass="column2">
```

```
</div>
```

```
<divclass="column2">
```

```
<h1>WelcomeToTPAPage</h1>
```

```
</div>
```

```
<br></br>
```

```
<h1>TPALogin</h1>
```

```
<formname="login"action="tpaloginaction.jsp"method="post">
```

```
<tablebgcolor="orange"style="margin-top:50px;width:300px;"
align="center">
```

```

<tr>

    <td><fontsize="4"color="green"style="">UserName</td>

    <td><inputtype="text"name="uname"required></input></td>

</tr>

<tr>

    <td><fontsize="4"color="green"style="">Password</td>

    <td><inputtype="password"name="password"required></input></td>

</tr>

<tr>

    <td><inputtype="Submit"value="Login"style="font-size:
15px;"></input></td>

    <td><inputtype="Reset"style="font-size:15px;"></input></td>

</tr>

</table>

</form>

</div>

<brclass="clear"/>

</div>

</div>

<divclass="wrappercol4">

    <divid="footer">

```

`</div>`

`<brclass="clear"/>`

`</div>`

`</div>`

`</body>`

`</html>`

## B. SCREENSHOTS

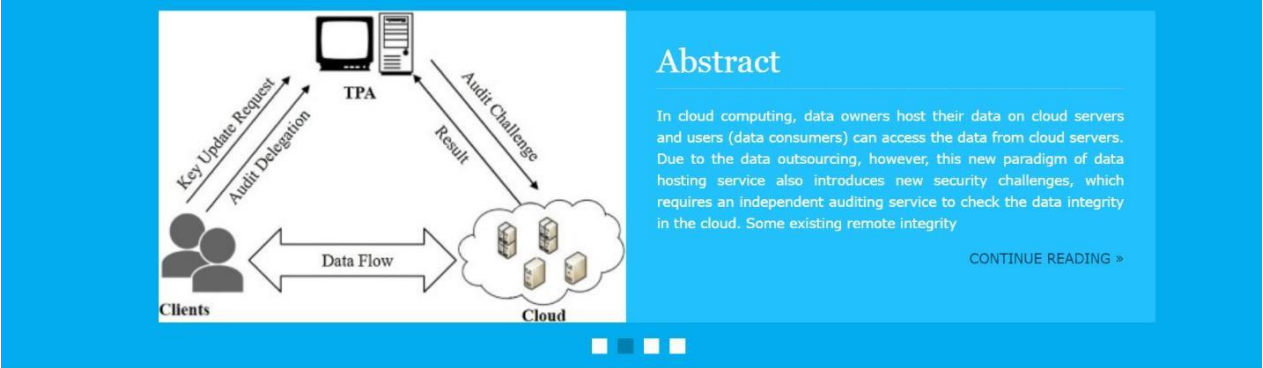
Welcome To Client Register

|                                         |                                                   |
|-----------------------------------------|---------------------------------------------------|
| First Name                              | <input type="text" value="williams"/>             |
| Last Name                               | <input type="text" value="raj"/>                  |
| Email ID                                | <input type="text" value="williams12@gmail.com"/> |
| Mobile Number                           | <input type="text" value="9876543210"/>           |
| Location                                | <input type="text" value="chennai"/>              |
| Complete Address                        | <input type="text" value="Chennai"/>              |
| User Name                               | <input type="text" value="williams"/>             |
| Password                                | <input type="password" value="*****"/>            |
| <input type="button" value="Register"/> | <input type="button" value="Reset"/>              |

***Fig5.1Loginpage***



***Fig5.2ClientRegistration***



Upload File Here

|                                       |                                                           |
|---------------------------------------|-----------------------------------------------------------|
| File ID                               | <input type="text" value="8"/>                            |
| Subject                               | <input type="text"/>                                      |
| Choose File                           | <input type="button" value="Choose File"/> No file chosen |
| <input type="button" value="Upload"/> |                                                           |

**Fig5.3UploadFile**



File Sending With Meta Key

| Blocks | Secrete Key          | Metadata Key | Status | Send                                |
|--------|----------------------|--------------|--------|-------------------------------------|
| Block1 | <input type="text"/> |              |        | <input type="button" value="Send"/> |

|                      |            |
|----------------------|------------|
| Each Block Size      | 10.6 Bytes |
| Total Size           | 53.0 Bytes |
| <a href="#">Back</a> |            |

**Fig5.4FileSendingMetaKey**



| Blocks                                  | Secret Key                      |
|-----------------------------------------|---------------------------------|
| Block1                                  | <input type="text" value="s1"/> |
| Block2                                  | <input type="text" value="s2"/> |
| Block3                                  | <input type="text" value="s3"/> |
| Block4                                  | <input type="text" value="s4"/> |
| Block5                                  | <input type="text" value="s5"/> |
| <input type="button" value="Download"/> |                                 |

***Fig5.5SecretKey***

Welcome to Client Home :hup@gmail.com

## DOWNLOAD HISTORY

| FileName | Downloaded Date     |
|----------|---------------------|
| demo.txt | 2024-03-23 14:41:00 |

***Fig5.6DownloadHistory***

## C. RESEARCH PAPER

# BLOCKCHAIN CLOUD BANKING: SECURE AND FAULT TOLERANT TRANSACTIONS

P. Navaneeth<sup>1</sup>

<sup>1</sup>Research Scholar, Department of Computer Science and Engineering, Sathyabama  
Institute of Science and Technology.

[navaneethsapna@gmail.com](mailto:navaneethsapna@gmail.com)

G. Balaji Bharath<sup>2</sup>

<sup>2</sup>Research Scholar, Department of Computer Science and Engineering,  
Sathyabama Institute of Science and Technology.

[balajibharath292003@gmail.com](mailto:balajibharath292003@gmail.com)

D. Nancy Kirupanithi<sup>3</sup>

<sup>3</sup>Assistant Professor, Department of Computer Science and Engineering, Sathyabama  
Institute of Science and Technology.

[nancykirupanithi.cse@sathyabama.ac.in](mailto:nancykirupanithi.cse@sathyabama.ac.in)

**Abstract:** Currently, it's far hard to hold and share records securely. A patron in a verbal exchange device sends its record in encrypted shape the use of a secret key. This belongings is essential for any excessive-level facts trade device, due to the fact every client that discloses sensitive statistics will make it hard for the owner of the information to maintain the safety of the information. This paper affords a schematic and effective release scheme, demonstrates its safety and implements to illustrate its rationality. Information owners make many attempts to share their information On servers or within the cloud. There are answers to

each of these questions. These techniques are important to manipulate the public key. owner records.

This record authorizes customers to get right of entry to cloud authentication information. The assumed authority makes use of the SHA calculation to generate the important thing, and the keys sent to the customer and owner. The believe report uses the MD-V set of rules to extract the fee after receiving the encrypted document from the data proprietor the use of the AES algorithm. It is used to research dynamic operation on its dataset and which system adjustments among huge facts stores. A send the authentication document to the

**CSP module to advantage get right of entry to the cloud.**

**Successful keyshave been shown to have many nice houses, making certain the confidentiality of correspondence from eavesdroppers from distinct nodes within the agency.**

**Keywords: Security, Encryption, Security, Private Key, Authenticate, Cloud**

## INTRODUCTION

When pronounced, the disbursed computing type demonstrates a re-evaluation of control, for that reason reshaping the distribution of power. Customers can use it results easily. They do not should fear about in which the power comes from, or how things are made and moved. They keep feeding. A similar concept underlies cloud computing: customers can use garage, computing strength, or a specially designed improvement environment with out stressful approximately how the entirety works domestically. A distributed laptop is often a internet-based totally MGE. Similar to cloud net, handiest internet is supplied on a PC community account;

In different words, dark discussion obscures Internet research. It is a computing method wherein bound features are furnished "as a service". It lets in users to get right of entry to technical offerings from the Internet ("inside the cloud") without the know-how and manipulate of the technical provider. Cloud logging can be located in big cloud environments and huge IT infrastructures, which constitute growing issues in having access to recorded information. Consequently reducing the contents in line with nature. Cloud computing has exceptional implications for cloud computing and big structures.

However, anotunusual detail that can be found is the issue of an appropriate distribution of content material, which is pushed by using making measurement to similarly enhance accuracy. The data plane and the manipulate aircraft make up the cloud deck.

For example, in an information platform, cloud logging allows procedure management to be at the threshold of the employer in place of servers in a server farm. Unlike dispensed computing, cloud computing is targeted on stop customers and target customers, with wide geographic distribution and consolidation of adjoining property, reducing downtime and monitoring community performance. This guarantees the high-quality exceptional. In case of frustration, acquainted experience and unexpected repetition also can be used in AAL situations.

## OBJECTIVE

The essential goal of the framework is to make sure that the assignment is fully and effectively launched to illustrate its safety, and is applied to illustrate its sustainability. The main cause of this gadget is that the SHA calculation is utilized by the legal individual. To generate a key, this key is dispatched to the client along with the owner. The force module receives an encrypted certificates from the product owner using AES computation and subtracts the price using MD-V computation.

## LITERATURE SURVEY:

### ***1. Effective and Undeniable Reviewing the layout plan Correlations***

With the rapid improvement of allotted computing, comfortable re-computation strategies have attracted growing attention from main researchers. revaluating calculation worldview, the clients with asset obliged capacities can re-appropriate the weighty calculation jobs into the cloud server and appreciate limitless processing assets in a compensation for each utilization way. Perhaps of the most basic usefulness in rethinking calculation is the undeniable nature of the outcome.

### ***2. Comparison rows can be adequately eliminated***

One of the most crucial aspects of outsourcing is validation.

However, there are some secure mechanisms for compatibility evaluation that permit clients to recognise whether servers surely put into effect the protocol or not. In this paper, we deal with this hassle with the aid of combining synthetic frameworks with homomorphic notation. Compared to present schemes, the proposed reaction allows our clients to efficiently hit upon server corruption.

### **3. Comparison of comfy and personal series**

The range of conversations in our protocol is proportional to the time complexity queue estimation algorithm. The hassle of determining sequence similarity happens in many files, particularly in bioinformatics. In these conversion programs, a rule of collections similarity is broadly used: the value the range of conversations in our protocol is proportional to the time complexity is minimal.

### **4. New Calculation for Secure Rethinking Particular Exponentiations**

Layers are considered the highest priced operations in cryptographic ensembles based totally on discrete logarithms. This paper proposes a new relaxed scaling set of rules for increasing the first blocks in a one-loop version. Compared to advanced systems, the Computational Proposition is unique in its artwork and its actual operation. Then, on this step, we use this computation as an exercising to assess the relaxed encryption of Cramer-Shop and Schnorr labels. It provides the primary comfy and productive approach of high-speed garage on the same time.

### **5. Y. Wan et al.**

developing a strategy for sharing medical information the use of a blockchain-based allotted computing method. Security and protection are maintained via authentication and various blocking off strategies. The simple shape of the assignment for the block chain supports the basic regions inclusive of organizational version, production data, and contractual instrument. The proposed method has simplest been examined at the Ethereum platform; because storing

and retrieving information from the cloud platform calls for more bandwidth, however this doesn't guarantee that it's going to carry out properly on exceptional architectures. Y. Zhu and et al. He proposed a framework to ease fact trading the use of closed discovery and overcoming the boundaries of present frameworks.

### **6. F. Deng et al. presented individual Wellbeing Record Trade utilizing Trait Based Signcryption**

They describe the structure of CP-OABSC, specifically based totally on the ABE diagram, which derives the encryption verification, however uses the signature verification server operation. As for the encryption approach used, you go., which uses qualified encryption to get right of entry to and show an correct, secure and dependable shape. Z. Wu et al.

### **7. Check and keep up with the medical services related clinical testaments of patients utilizing savvy contracts**

As defined within the "Rationale and Limitation" section, block findings are utilized by experts in various international locations. The complete idea changed into to use the technology to limit intrusions into the IoT machine. In order to cozy access to fitness records, creators brought numerous declarations of authority (CA).

In order to make certain the security of IoT gadgets, a easy affirmation method is usually recommended, which ensures inertia and in addition will increase compliance measures and information retention.

### **8. To check the clinical**

The capability to check in a scientific claim and show it became difficult in a traditional framework like Industry four.0, this hassle has been solved with the help of Internet of Things, Blockchain, Artificial Intelligence and plenty of different superior innovations. The authors introduce two strategies (node-primarily based connectivity and safety evaluation) for sophisticated complex structures to capture

nodes from diverse neighborhood authentication computations.

#### **9. F. Deng et al. presented individual Wellbeing Record Trade utilizing Quality Based Signcryption**

In general, the CP-OABSC system is predicated on ABE maps and decodes to verify it, however signature verification is supported by the server.

A cross-encryption system is used, which makes use of a requirements-primarily based technique to encryption and demonstrates an accurate, cozy and dependable structure. Z.

Wu et al. Proposed a totally well matched bilinear-based totally cryptosystem that makes use of 4 encryption and decryption models.. People simplest want to store one private key to get extraordinary keys.

#### **10. The medical care framework has been worked on after the reception of developing innovation like the Web of Things (IoT), Edge Computing, Artificial Intelligence, AI,**

However, the protection and safety of records related to clinical offerings nevertheless stays a project. It consists of critical and sensitive statistics about patients and if any records is contained or leaked thru recent cybercriminal attacks it can be very dangerous for patient's lifestyles.

Therefore, experts have proposed several strategies to track and shop facts approximately medical services. B. Schickel et al. They offer a precis of the maximum advanced getting to know-based totally approaches utilized in clinical programs for EHR research. The authors describe the constraints of existing systems and fashions carried out to heterogeneous records;

#### **EXISTING SYSTEM**

Enormous challenges within the bodily and natural sciences are being addressed by means of traits in on line processing, consisting of pass-sectional computing, that allow huge adjustments in memory, speed, storage, and records. The susceptible restore engine related to such an affiliation is usually not restrained by way of its gradual

velocity, hidden storage capacity, and restrained statistics mobility: it could use the abundance of these sources to behave some place else in the association. The use of "factor allocation" is complex through the truth that the facts in question are frequently exceptionally private, along with information vital to public fitness, different and patented innovations, or that must be kept personal because of felony requirements. HIPAA Gram. -Bily filter or comparable regulations. It permits a comfortable way, that is, it enables the making plans of enterprise laptop systems, without the outcomes of calculations of very own data or data to professionals a long way away from the place wherein the laptop gadget is used.

#### **Disadvantages of Existing System**

1. Outsourcing solutions are extensively relevant to the following procurement problems.
2. The largest danger of this intel

#### **PROPOSED SYSTEM**

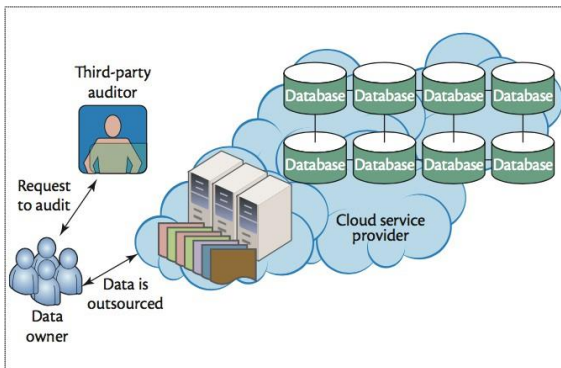
We advocate a convenient trade scheme that allows you to with no trouble distribute keys and exchange notes for dynamic meetings. We offer a handy region for key change without one time a hard and fast correspondence channel. Clients can affirm the purchaser's public key to securely retrieve non-public keys from an untrusted purchasing agent. Our software program can perform nice-grained get right of entry to manipulate; By gathering a list of customers, any client within the group can use the cloud resource, and remote clients cannot get entry To the cloud after retreat. We have a comfortable registry that protects the safety of communications in opposition to conspiracy assaults. Regardless of whether clients cooperate with the untrusted cloud or no longer, they cannot get better previously discarded data. Using our approach, the customer can get complete profits. Our software can efficiently help effective organizations; If another purchaser joins a assembly or a client is removed from a meeting, the machine is forced to recalculate or replace the diverse private keys of

the customers. We conduct safety research to illustrate our protection desires.

### **Advantages of Proposed System**

1. Power Method for Influence and control
2. More determination
3. Safer and extra productive.
4. Confidential Information.

### **SYSTEM ARCHITECTURE**



### **MODULES**

Using 5 extraordinary blocks

1. Login Module
2. Enrolment Module
3. Creation Capacity and Occurrence
4. Trackdown conspiracy Module
5. Trackdown Outsider Module

#### **1. Login Module**

This setting may be very important, customer ought to offer accurate touch number and password which consumer enters for the duration of registration in registration software. Assuming the client's records match the records in the card table that is honestly the document in use,

otherwise a failure message should be opened and an appropriate facts again to the consumer. A link to registration hobby is also carried out to attract new clients.

**Input:** Username and Password

**Output:** Admin Login

#### **2. Enrolment Module**

Another consumer this setting is very critical, patron ought to provide accurate touch range and utility must first check in before logging in. When you input your email address within the login manner, the registration function will open. Another consumer registered by means of entering his complete name, password and speak to range. The client need to re-enter the password. Enter the confirmation password for the verification subject. At this point, when the patron enters the information in all the content fields; clicking register moves the facts to the required records and the purchaser is again incorporated with the login action.

**Input:** Username and Password

**Output:** Database

#### **3. Creation Capacity and Occurrence**

Enter the affirmation password for the verification subject. At this point, when the patron enters the records in all of the content material fields;

**Input :** Username and Password

**Output:** data uploaded

#### **4. Trackdown conspiracy Module**

Using distance calculations, a receiver on this block can decide whether collusion has passed off.

**Input:** Username and Password

**Output:** Database

#### **5. Trackdown Outsider Module**

In this module, the collector also can track foreigners. External refers to any other entity within the first seller's software.

**Input:**UserNameandPassword

**Output:** find third-parties

## SYSTEM REQUIREMENTS

### HardwareRequirements:

System:Pentium-IV

Speed: 2.4GHZ

Hard disk: 40GB

Monitor:15VGAcolour RAM:

512MB

### SoftwareRequirements:

OperatingSystem:WindowsXP

Coding language: Java

IDE: Net beans

Database:MYSQL



## RESULTANDDISCUSSION

### SCREENSHOTS

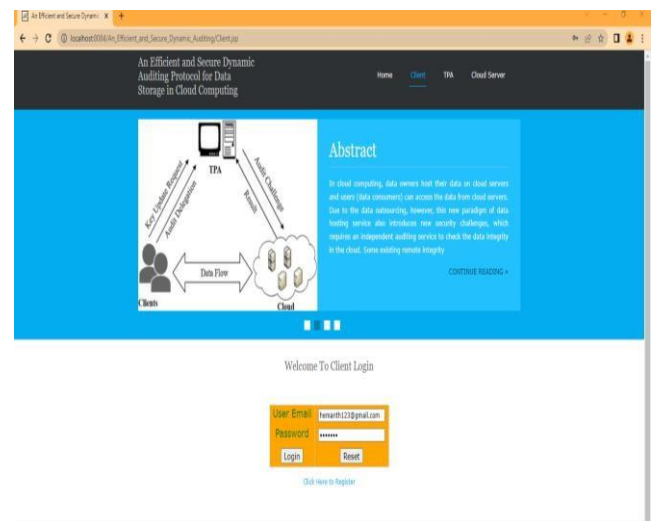
#### Home Page



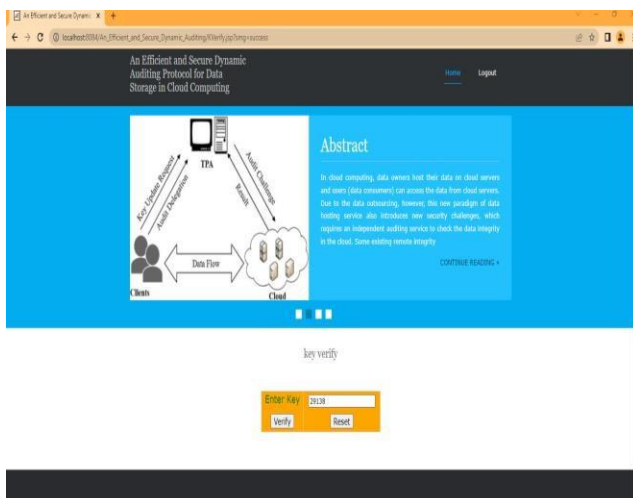
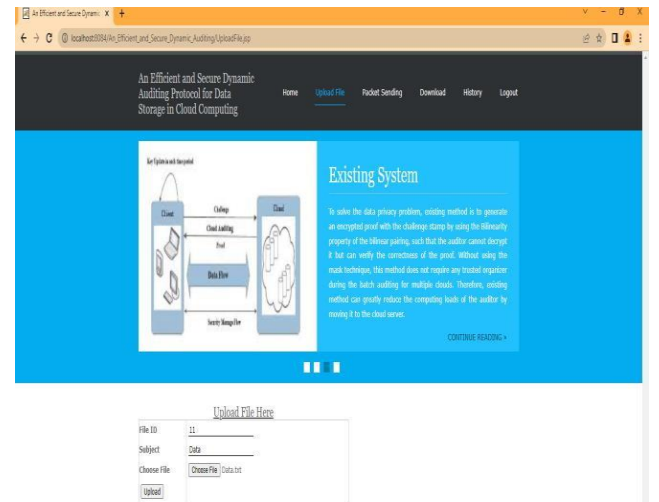
**Abstract**

In cloud computing, data owners host their data on cloud servers and users (data consumers) can access the data from cloud servers. Due to the data outsourcing, however, this new paradigm of data hosting service also introduces new security challenges, which require an independent auditing service to check the data integrity in the cloud. Some existing remote integrity checking methods can only serve for static archive data and thus cannot be applied to the auditing service since the data in the cloud can be dynamically updated. Thus, an efficient and secure dynamic auditing protocol is desired to convince data owners that the data are correctly stored in the cloud. This paper first designs an auditing framework for cloud storage systems and proposes an efficient and privacy-preserving auditing protocol. Then, this will be extended for auditing protocol to support the data dynamic operations, which is efficient and provably secure in the random oracle model. Further the auditing protocol is extended to support batch auditing for both multiple owners and multiple clouds, without reuse new trusted resources. The analysis and simulation

#### ClientLoginPage



#### ClientRegistrationPage



## UploadFile

Advocate a secure record sharing scheme that will allow clean distribution of keys and exchange of information for dynamic conferences. Provide us appropriate approach for changing keys without a set correspondence channel. Clients can verify the purchaser's public key to securely retrieve personal keys from an untrusted shopping agent. Our software can perform high-quality, graded admission to control; by amassing a listing of clients, Any customer inside the employer can use the powerful assist of the cloud, and faraway customers can't get admission to the cloud left at the

back of. We offer well timed touch coverage that protects in opposition to conspiracy attacks.

Regardless of whether clients cooperate with the untrusted cloud or not, they can't get better previously discarded records.

Using our strategy, the customer can get full income. Our software can efficaciously guide effective companies; if any other consumer joins a meeting or a customer is eliminated from a meeting, the machine is forced to recalculate or update the diverse personal keys of the clients. We conduct safety studies to illustrate our safety dreams.

#### FUTURE SCOPE

This will help ensure that the user can easily get entry to regularly used documents at any time. Additionally, a credit score system may be added where in every node is assigned a default of one hundred credits based totally on their machine uptime, and multiple successful document calls can lower or growth their credits. A person with more credits may be given higher priority at the same time as saving statistics.

#### REFERENCES

- [1] Y. Feng, H. Ma, and X. Chen, "Efficient and verifiable outsourcing scheme of sequence comparisons," *Intell. Autom. Soft Comput.*, vol. 21, no. 1, pp. 51–63, Jan. 2015.
- [2] M. J. Atallah and J. Li, "Secure outsourcing of sequence comparisons," in *Proc. Int. Workshop Privacy Enhancing Technol. (PET)*, Toronto, ON, Canada, 2004, pp. 63–78.
- [3] M. J. Atallah, F. Kerschbaum, and W. Du, "Secure and private sequence comparisons," in *Proc. ACM Workshop Privacy Electron. Soc. (WPES)*, Washington, DC, USA, 2003, pp. 39–44.
- [4] D. Szajda, M. Pohl, J. Owen, and B. Lawson, "Toward a practical data privacy scheme for a distributed implementation of the Smith-Waterman genome sequence comparison algorithm," in *Proc. Netw. Distrib. Syst. Secur. Symp. (NDSS)*, San Diego, CA, USA, 2006, pp. 253–265.
- [5] X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, "New algorithms for secure outsourcing of modular exponentiations," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 9, pp. 2386–2396, Sep. 2014.
- [6] R. Akimane, O. Markowitch, and Y. Roggeman, "Secure outsourcing of DNA sequences comparisons in a Grid environment," *WSEAS Trans. Comput. Res.*, vol. 2, no. 2, pp. 262–269, Feb. 2007.
- [7] M. Blanton, M. J. Atallah, K. B. Frikken, and Q. Malluhi, "Secure and efficient outsourcing of sequence comparisons," in *Proc. Eur. Symp. Res. Comput. Secur. (ESORICS)*, Pisa, Italy, 2012, pp. 505–522.
- [8] Y. Feng, H. Ma, X. Chen, and H. Zhu, "Secure and verifiable outsourcing of sequence comparisons," in *Proc. Int. Conf. Inf. Commun. Technol. (ICT-EurAsia)*, Yogyakarta, Indonesia, 2013, pp. 243–252.
- [9] S. Salinas, X. Chen, J. Li, and P. Li, "A tutorial on secure outsourcing of large-scale computations for big data," *IEEE Access*, vol. 4, pp. 1406–1416, Apr. 2016.
- [10] X. Chen, J. Li, J. Weng, J. Ma, and W. Lou, "Verifiable computation over large database with incremental updates," *IEEE Trans. Comput.*, vol. 65, no. 10, pp. 3184–3195, Oct. 2016.
- [11] Medshare: a novel hybrid cloud for medical resource sharing among autonomous healthcare providers *IEEE Access*, 6(2018), pp. 4694946961, 10.1109/ACCESS.2018.2865535(2021)
- [12] F. Deng, Y. Wang, L. Peng, H. Xiong, J. Geng, Z. Qin, "Ciphertext-policy attribute-based signcryption with verifiable outsourced designcryption for sharing personal health records," *IEEE Access*, vol. 6(2020), pp. 39473–39486, 10.1109/ACCESS.2018.2843778
- [13] Z. Wu, "Group-oriented cryptosystem for personal health record exchange and sharing," *IEEE Access*, vol. 7(2019), pp. 146495–146505, 10.1109/ACCESS.2019.2946266

- [14] L. Ismail, H. Materwala, S. Zeadally, "Lightweight blockchain for healthcare," *IEEE Access*, vol. 7 (2019), pp. 149935-149951, 10.1109/ACCESS.2019.2947613
- [15] A. Shahnaz, U. Qamar, A. Khalid, "Using blockchain for electronic health records," *IEEE Access*, vol. 7 (2019), pp. 147782-147795
- [16] Yogesh Sharma, B. Balamurugan, "Preserving the privacy of electronic health records using blockchain," *Proc. Comput. Sci.*, 173 (2020), pp. 171-180, 10.1016/j.procs.2020.06.021
- [17] C. Pirtle, J. Ehrenfeld, "Blockchain for healthcare: the next generation of medical records?" *J. Med. Syst.*, 42 (2018), p. 172, 10.1007/s10916-018-1025-3
- [18] Sara Saberi, Mahtab Kouhizadeh, Joseph Sarkis, Lejia Shen, "Blockchain technology and its relationship to sustainable supply chain management" (2022)
- [19] P. Treleaven, R. Gendal Brown, D. Yang, "Blockchain technology in finance," *Computer*, vol. 50 (2022), pp. 14-17, 10.1109/MC.2017.3571047
- [20] Sudeep Tanwar, Karan Parekh, Richard Evans, "Blockchain-based electronic health care records system for healthcare 4.0 applications," *J. Inf. Secur. Appl.*, 50 (2020), Article 102407
- [21] E. Daraghmi, Y. Daraghmi, S. Yuan, "MedChain: a design of blockchain-based system for medical records access and permissions management," *IEEE Access*, vol. 7 (2019).
- [22] N. Samwel, L. Batina, "Practical fault injection on deterministic signatures: the case of EdDSA," *Prog. Cryptol. – AFRICACRYPT 2018 Lecture Notes in Comp. Sci.* (2020), pp. 306-321
- [23] Aitizaz Ali, et al. "Security, privacy, and reliability in digital health care systems using blockchain," *Electronics*, 10 (16) (2021), p. 2034
- [24] Aitizaz Ali, et al. "Deep learning based homomorphic secure search-able encryption for keyword search in blockchain healthcare system: a novel approach to cryptography," *Sensors*, 22 (2) (2022), p. 528
- [25] Aitizaz Ali, et al. "An industrial IoT-based blockchain-enabled secure search-able encryption approach for healthcare systems using neural network," *Sensors*, 22 (2) (2022), p. 572

# CONFERENCE CERTIFICATE

